IJW
AT

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Serial No.: 09/944,996

Filing Date: 8/31/2001

Applicant(s): Brian K. Martin

Entitled: STATE MACHINE FOR ACCESSING A STEALTH FIREWALL

Group Art Unit: 2135

Attorney Docket No.: RSW920010151US1 (7161-9U)

CERTIFICATE OF MAILING

I hereby certify that the following documents are being deposited with the United Sates Postal Service in an envelope with sufficient postage as first-class mail addressed to: Mail Stop Appeal Brief – Patents, Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on February 21, 2006

- Appeal Brief (23 pgs)
- Transmittal letter
- Return receipt postcard

Respectfully submitted,

Peggy Shock

Peggy Shock, Legal Assistant to
Steven M. Greenberg
Registration No. 44,725
Christopher & Weisberg, P.A.
200 East Las Olas Boulevard, Suite 2040
Fort Lauderdale, FL 33301

50219

Docket No. RSW920010151US1 (7161-009U) **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number:	09/944,996
Filing Date:	August 31, 2005
Appellant(s):	Brian MARTIN
Entitled:	STATE MACHINE FOR ACCESSING A STEALTH FIREWALL
Examiner:	L. Ha
Group Art Unit:	2134
Attorney Docket No.:	RSW920010151US1 (7161-009U)

TRANSMITTAL OF APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

Submitted herewith is Appellant's Appeal Brief in support of the Notice of Appeal filed December 2, 2005, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review dated January 19, 2006.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due under 37 C.F.R. §§ 1.17, 41.20, and in connection with the filing of this paper, including extension of time fees, to Deposit Account 09-0461, and please credit any excess fees to such deposit account.

Date: February 21, 2006

Respectfully submitted,

Scott D. Paul, Registration No. 42,984
Christopher & Weisberg, P.A.
200 E. Las Olas Blvd., Suite 2040
Fort Lauderdale, FL 33301
Tel: (954) 828-1488
Facsimile: (954) 828-9122

Docket No. RSW920010151US1 (7161-009U) **PATENT**

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

Application Number:	09/944,996
Filing Date:	August 31, 2005
Appellant(s):	Brian MARTIN
Entitled:	STATE MACHINE FOR ACCESSING A STEALTH \ FIREWALL
Examiner:	L. Ha
Group Art Unit:	2134
Attorney Docket No.:	RSW920010151US1 (7161-009U)

APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Appeal Brief is submitted in support of the Notice of Appeal filed December 2, 2005, and in response to the Notice of Panel Decision from Pre-Appeal Brief Review dated January 19, 2006, wherein Appellant appeals from the Examiner's rejection of claims 1-13.

I. REAL PARTY IN INTEREST

This application is assigned to IBM Corporation by assignment recorded on August 31, 2001, at Reel 012146, Frame 0346.

II. RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any related appeals and interferences.

III. STATUS OF CLAIMS

Claims 1-13 are pending in this Application. Of those, claims 1-13 have been finally rejected, and it is from the final rejection of claims 1-13 that this Appeal is taken.

IV. STATUS OF AMENDMENTS

The claims have not been amended subsequent to the imposition of the Final Office Action dated October 7, 2005.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Referring to independent claims 1 and 7-13 and Figure 2 of Appellant's disclosure, a stealth firewall 210 receives network requests 280 from a network device 230 for access to a protected network 270 (page 11). Referring also to Figures 3A and 3B, the stealth firewall 210 includes a state machine 250 that transitions across a plurality of states. These states may include a restricting state, and intermediate state, and an access state. In the restricting state, the firewall 210 may not respond to any request 280 (page 12), and in the access state, the firewall 210 allows access to the protected network 270.

The state machine 250 transitions from one state to another state based upon a plurality of network requests 280 from the network device 230. Each request 280 acts as a portion of a code, and the plurality of requests 280 (producing a plurality of portions of the code) collectively comprise the code for causing the state machine 250 from the restricting state to the access state.

As stated on page 14 of Appellant's disclosure "the state machine behaves analogously to a combination lock wherein the combination is comprised of the various values represented by Code 1, Code 2, ..., Code n-1, Code n."

VI. ISSUES TO BE REVIEWED ON APPEAL

1. Claims 1-9 and 11-13 were rejected under 35 U.S.C. § 102 for anticipation upon Reid et al., U.S. Patent No. 6,182,226 (hereinafter Reid); and

2. Claim 10 was rejected under 35 U.S.C. § 102 for anticipation based upon Rothermal et al., U.S. Patent No. 6,678,827 (hereinafter Rothermal).

VII. THE ARGUMENT

THE REJECTION OF CLAIMS 1-9 AND 11-13 UNDER 35 U.S.C. § 102 FOR ANTICIPATION BASED UPON REID

For convenience of the Honorable Board in addressing the rejections, dependent claims 2-6 stand or fall together with independent claim 1, independent claim 11 stands or falls together with independent claim 7, independent claim 12 stands or falls together with independent claim 8, and independent claim 13 stands or falls together with independent claim 9.

Failure to Establish Reid Identically Discloses Each of the Claimed Elements

The factual determination of anticipation under 35 U.S.C. § 102 requires the identical disclosure, either explicitly or inherently, of each element of a claimed invention in a single

reference.[1] As part of this analysis, the Examiner must (a) identify the elements of the claims, (b) determine the meaning of the elements in light of the specification and prosecution history, and (c) identify corresponding elements disclosed in the allegedly anticipating reference.[2] This burden has not been met. Moreover, the Examiner has failed to clearly designate the teachings in Reid being relied upon the statement of the rejection. In this regard, the Examiner's rejection under 35 U.S.C. § 102 also fails to comply with 37 C.F.R. § 1.104(c).[3]

Evidence of the Examiner failing to comply with the requirements of 37 C.F.R. § 1.104(c) is found in the Examiner's own comments. On page 4 of the Final Office Action, the Examiner stated the following:

> Although the examiner may point to one or two citations in the last rejection, the rejection is not only limited to what was cited but that the entire reference (Reid, et al.) should provide more details and explanations to the rejected claims.

As readily apparent from the Examiner's own comments, the Examiner has not "designated as nearly as practicable" the particular parts in Reid being relied upon in the rejection, as required by 37 C.F.R. § 1.104(c). Instead, the Examiner is improperly placing the burden on Appellant to establish that Reid does not disclose the claimed elements based upon Appellant's interpretation of the claims and Appellant's comparison of the claims with the applied prior art. However, this shifting of burden, from the Examiner to Appellant, is premature since the Examiner has not discharged the initial burden of providing a *prima facie* case of anticipation.

---

[1] In re Rijckaert, 9 F.3d 1531, 28 USPQ2d 1955 (Fed. Cir. 1993); Lindermann Maschinenfabrik GMBH v. American Hoist & Derrick Co., 730 F.2d 1452, 221 USPQ 481 (Fed. Cir. 1984).
[2] Lindermann Maschinenfabrik GMBH v. American Hoist & Derrick Co., supra.
[3] 37 C.F.R. § 1.104(c) provides:

> In rejecting claims for want of novelty or for obviousness, the examiner must cite the best references at his or her command. When a reference is complex or shows or describes inventions other than that claimed by the applicant, the particular part relied on must be designated as nearly as practicable. The pertinence of each reference, if not apparent, must be clearly explained and each rejected claim specified.

For example, independent claim 1 recites:

> a state machine pre-configured to transition across a plurality of internal states, from a restricting state to an access state, conditioned upon receiving a plurality of requests to access said internal network. (emphasis added)

On pages 8-9 of the Amendment filed June 13, 2006 (hereinafter Amendment), Appellant argued that the statement of the rejection fails to clearly identify many of the specific elements within Reid being relied upon in the rejection. In particular, while referring to the above-identified language found in claim 1, Appellant noted that Examiner merely repeated the above-identified claim language word-for-word and asserted that these features are identically disclosed in column 5, line 58 through column 6, line 40. Appellant also argued that the Examiner failed to specifically identify within Reid the disclosed elements corresponding to the following claimed features: (i) a state machine; (ii) a plurality of internal states; (iii) a restricting state; (iv) a plurality of requests to access an internal network; and (v) an access state. However, despite Appellant's argument that the Examiner has failed to specifically identify all of the claimed limitations, the Examiner has not cured this failure in the Final Office Action. Thus, the Examiner's rejection fails to meet the requirements of both 35 U.S.C. § 102 and 37 C.F.R. § 1.104(c).

Independent Claim 1

As evident from the plain language of claim 1, a plurality of requests to access the internal network are required before the state machine transitions from a restricting state to an access state. In contrast, Reid discusses that several nodes in a decision tree are used when

making a decision about a connection (column 5, lines 64-67). Reid further states that "[e]ach node is compared against an incoming connection request and you determine whether the connection is allowed or denied based on the results of the node comparison" (column 6, lines 5-8). Thus, a connection decision is made by Reid based upon a single incoming connection request, and not a plurality of requests, as recited in claim 1.

The Examiner responded to this argument on pages 3 and 4 of the Final Office Action. Although not entirely clear, the crux of the Examiner's argument appears to be that "[t]he claim language states plurality of requests where Reid reads on having many users/groups or packets requesting access." This assertion by the Examiner ignores Appellant's arguments and the plain language of the claim 1, which recites:

> said plurality of requests collectively comprising a code for causing said state machine to transition from said restricting state to said access state which causes said packet filter to permit access to said internal network.

The Examiner, however, has failed to establish where Reid teaches a plurality of requests **collectively** comprise a code, and there is no teaching within Reid that the plurality of users/groups sending a plurality of requests collectively comprise a code. Instead, as already argued above, "a connection decision is made by Reid based upon a single incoming connection request, and not a plurality of requests." Whereas Reid teaches a plurality of requests (each ensuing in a separate connection decision) thereby creating a plurality of connections decisions, the claimed invention recites that a plurality of requests (collectively comprising a code) are needed to result in a single connection decision.

Appellant further notes that claim 1 also recites:

> said packet filter not responding to said external network upon receiving any request from said external network to access said internal network when said state machine in said restricting state (emphasis added).

This limitation was added in the Amendment, and Appellant argued that column 12, lines 56-59 of Reid states that a failure code is not returned if a password was not accepted, and Reid states in column 15, lines 61-64 that a ping is responded to "if ping response is enabled for the region from which the packet came." This teaching within Reid, however, is not comparable to the packet filter not responding to any request from an external network when the state machine is in a restricting state. The conditions for responding (i.e., password accepted, region enabled) disclosed by Reid are found in the current connection request, whereas the claimed state condition of the state machine is based on information contained in a prior connection request. Therefore, Reid further fails to identically disclose the claimed invention, as recited in claim 1, within the meaning of 35 U.S.C. § 102.

On page 7 of the Final Office Action, the Examiner asserted that this feature is identically disclosed in column 15, lines 11-13 and 61-63. These passages are reproduced below:

> If the connection is not allowed, then the counters are automatically freed up and the proxy need not make any further calls for that connection. (column 15, lines 11-13)
>
> In the ICMP (Internet Control Message Protocol) processing, if the incoming packet is an ICMP ECHO_REQUEST (commonly known as a "ping"), check the region table and only respond if ping response is enabled for the region from which the packet came. (column 15, lines 59-63)

The Examiner also stated the following in the paragraph spanning pages 4 and 5:

> **In regards to the argument of not responding to the request:** no response or ignores to requests in the restricting state is where Reid discloses the connection is not allowed therefore need not make any further calls for that connection. Further, Reid discusses only to respond to the incoming packet which is the request if the region table indicates that the ping is enabled. Thus, it

is inherent to not respond to the packet if the region table indicates the ping is disabled. (col. 15, lines 11-13 and 61-63). (emphasis in original)

The above-identified claimed limitation is directed to the operation of the packet filter when "said state machine in said restricting state." However, as previously noted, the Examiner has not identified (or distinguished between) those features that identically disclose the claimed "restricting state" and those features that identically disclose the claimed "access state" of the state machine. Moreover, even *assuming arguendo* that heretofore unidentified state machine of Reid is in the restricting state, the Examiner has not identified within Reid how the state machine transitions from the restricting state to the access state.

As recited in claim 1, the state machine makes this transition "conditioned upon receiving a plurality of requests ... collectively comprising a code for causing said state machine to transition from said restricting state to said access state." The teachings of Reid cited by the Examiner do not disclose that any request from an external network is not responded to based upon the state (i.e., a restricting state) of a state machine. Instead, Reid teaches that certain pings may be responded to based upon whether a region table indicates that a ping is enabled. Therefore, the transition, within Reid, from not responding to any request to responding to a request is based upon whether a region table indicates that a ping is enabled and not based upon a plurality of requests collectively comprising a code, as recited in claim 1. Thus, Reid further fails to identically disclose the claimed invention, as recited in claim 1, within the meaning of 35 U.S.C. § 102.

Claims 7 and 11

Similar to independent claim 1, independent claims 7 and 11 also recite the following claimed features: (i) a state machine; (ii) a plurality of internal states; (iii) a restricting state; (iv) a plurality of requests to access an internal network; and (v) an access state. Independent claims 7 and 11 also recite (vi) an intermediate state. The Examiner, however, has failed to clearly identify the specific elements within Reid being relied upon in the rejection that correspond to these claimed limitations.

Regarding claims 7 and 11, on page 11 of the Amendment, Appellant argued that a "review of this cited passage does not reveal any teaching of a second request, which in addition to a first request, is used to transition the state machine into a final state passage." On page 4 of the Final Office Action that Examiner cited column 14, lines 43-47 and asserted that "[t]he second call is the final state transition." The Examiner appears to have pulled this interpretation out of thin air since the Examiner has **failed to put forth any analysis and/or explanation** as to why one having ordinary skill in the art would recognize that the "second call" described by Reid corresponds to the claimed "transitioning from an intermediate state in said state machine to a final state if said identified further access request satisfies transitioning criteria associated with said state machine for transitioning from an intermediate state to said final state." In this regard, Appellant submits that the Examiner has improperly asserted that a single disclosed feature in Reid identically discloses a more complex limitation involving several features. Therefore, Reid fails to identically disclose the claimed invention, as recited in claims 7 and 11, within the meaning of 35 U.S.C. § 102.

Claims 8 and 12

On page 12 of the Amendment, Appellant argued that claims 8 and 12 recite "identifying access request parameter in said received access requests" and "performing state transitions in a state machine ... based upon identifying particular ones of said identified access request parameters." Similar to the language found in claims 7 and 11, this claim language recited in claims 8 and 12 is directed to using information from multiple requests to transition the state machine. This concept, however, is neither taught nor suggested by Reid. On pages 5 and 8 of the Office Action, the Examiner cited column 5, lines 58-63 and column 7, lines 34-51 and asserted that these citations disclose the above-identified claimed limitations. The citation in column 5 only regards the use of access rules "that matches the characteristics of the connection request [] to determine whether the connection should be allowed or denied." Thus, as already noted above, Reid teaches that information contained in a single connection request is used to determine access request. The citation in column 7 is only a list of various access rules that can be employed and fails to discuss using information in multiple connection requests to transition a state machine into a new state.

The Examiner did not directly address these arguments in the Final Office Action. Instead, the Examiner cited additional passages within Reid and asserted that "the plurality of requests as disclosed by Reid are users or users of different groups or data packets entering attempting to a connection to the second network," which is similar to the Examiner's prior comments regarding claim 1. This statement by the Examiner, however, exemplifies the distinction between the claimed invention and the teachings of Reid.

Claim 8 further recites:

> upon identifying a pre-determined sequence of access request parameters, said identification of said sequence of access request parameters causing a corresponding sequence of state transitions in the said machine, permitting access to a selected network device responsible for transmitting said sequence of access requests parameters. (emphasis added)

Although the Examiner asserts that the plurality of requests disclosed by Reid are "users or users of different groups or data packets entering attempting to a connection to the second network," the Examiner has failed to establish that Reid discloses that a selected network device (i.e., a single device) is responsible for transmitting a sequence of access requests parameters (which are identified in the received access requests). Instead, the Examiner is asserting that multiple entities are transmitting the access requests. Therefore, Reid fails to identically disclose the claimed invention, as recited in claims 8 and 12, within the meaning of 35 U.S.C. § 102.

Claims 9 and 13

On page 13 of the Amendment, Appellant argued that claims 9 and 13 recite that the "state machine transitioning through a plurality of states based upon a sequence of access request parameters identified in received access requests from a single network device." Again, similar to claims 7-8 and 12-13, claims 9 and 13 using request parameter identified in multiple requests to transition the state machine. To teach this feature, the Examiner cited column 16, lines 20-65 of Reid. This cited section of Reid refers to Fig. 5 and is entitled "Region Determination Processing." As evident from Fig. 5 and from the cited language, request parameters identified

in a plurality of access requests are not obtained. Instead, Reid states that information from a single request is used to determine whether the packet is forwarded or not.

The Examiner did not directly address these arguments in the Final Office Action. Instead, the Examiner cited additional passages within Reid and asserted that "the plurality of requests as disclosed by Reid are users or users of different groups or data packets entering attempting to a connection to the second network." Similar to claim 8, this statement by the Examiner exemplifies the distinction between the claimed invention and the teachings of Reid.

Claim 9 further recites:

> configuring a state machine to grant access to the stealth firewall contingent upon said state machine transitioning through a plurality of states based upon a sequence of access request parameters identified in received access requests from a single network device. (emphasis added)

Although the Examiner asserts that the plurality of requests disclosed by Reid are "users or users of different groups or data packets entering attempting to a connection to the second network," the Examiner has failed to establish that Reid discloses that a single network device provides the access requests from which a sequence of access request parameters are identified. Instead, the Examiner is asserting that multiple entities are transmitting the access requests. Therefore, Reid fails to identically disclose the claimed invention, as recited in claims 9 and 13, within the meaning of 35 U.S.C. § 102.

THE REJECTION OF CLAIM 10 UNDER 35 U.S.C. § 103 FOR ANTICIPATION BASED UPON ROTHERMAL

For convenience of the Honorable Board in addressing the rejections, claim 10 stands or falls alone.

Claim 10 recites that a comparator causing a packet filter to permit access where "said hashed password and timestamp matches said hashed result." Upon reviewing the Examiner's cited passages within Rothermal, Appellant notes that Rothermal fails to teach using the comparison of a hashed result to a hashed password in addition to a timestamp. Rothermal discusses the use of hashed passwords and separately discusses the use of a time stamp, but Rothermal fails to teach or suggest using a combination of hashed password and timestamp.

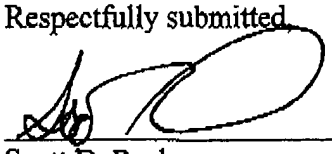
The Examiner responded to this argument on page 5 of the Final Office Action. Notwithstanding the Examiner's comments that "time stamp is one of the security information it is part of the security policy of the particular packet," a review of the Examiner's cited portions of Rothermal fails to yield a teaching of "said hashed password and timestamp matches said hashed result." Thus, Appellant submits that the Examiner has failed to establish a prima facie case of anticipation within the meaning of 35 U.S.C. § 102.

Conclusion

Based upon the foregoing, Appellant respectfully submits that the Examiner's rejections under 35 U.S.C. § 102 for anticipation based upon the applied prior art is not viable. Appellant, therefore, respectfully solicits the Honorable Board to reverse the Examiner's rejections under 35 U.S.C. § 102.

Date: February 21, 2006

Respectfully submitted,



Scott D. Paul
Registration No. 42,984
Steven M. Greenberg
Registration No. 44,725
Christopher & Weisberg, P.A.
200 E. Las Olas Blvd., Suite 2040
Fort Lauderdale, FL 33301
Tel: (954) 828-1488
Facsimile: (954) 828-9122

VIII. CLAIMS APPENDIX

1. A stealth firewall comprising:

a first network interface to an external network;

a second network interface to an internal network;

a packet filter for restricting access to said internal network; and,

a state machine pre-configured to transition across a plurality of internal states, from a restricting state to an access state, conditioned upon receiving a plurality of requests to access said internal network, said plurality of requests collectively comprising a code for causing said state machine to transition from said restricting state to said access state which causes said packet filter to permit access to said internal network, wherein

said packet filter not responding to said external network upon receiving any request from said external network to access said internal network when said state machine in said restricting state.

2 The stealth firewall of claim 1, wherein said requests from said external network comprise transport control protocol (TCP) SYN messages.

3 The stealth firewall of claim 2, wherein each state in said state machine corresponds to data in a specified field of said TCP SYN messages.

4 The stealth firewall of claim 3, wherein said specified field comprises a destination port field.

5 The stealth firewall of claim 1, wherein said code is a rolling code which can vary according to time.

6 The stealth firewall of claim 2, wherein said packet filter can permit access to a specific port in said internal network based upon a destination port specified in a TCP SYN message received after transitioning to said access state in said state machine.

7 A method for permitting access to a network protected behind a stealth firewall comprising the steps of:

initializing a state machine configured to grant access to the stealth firewall contingent upon said state machine transitioning across a plurality of internal states responsive to receiving a plurality of requests to access the network from a single network device, said plurality of requests collectively comprising a code for causing said state machine to permit access to the network;

receiving an access request from a network device in a network which is external to the network protected behind the stealth firewall, identifying an access parameter in said access request and transitioning from an initial state in said state machine to an intermediate state if said identified access request satisfies transitioning criteria associated with said state machine for transitioning from said initial state to said intermediate state;

receiving a further access request from said network device in said network which is external to the network protected behind the stealth firewall, identifying a further access parameter in said further access request and transitioning from an intermediate state in said state

machine to a final state if said identified further access request satisfies transitioning criteria associated with said state machine for transitioning from an intermediate state to said final state;

not providing a response to said network device upon receiving each said access request from said network device in said network which is external to the network protected behind the stealth firewall unless said network device provides a sequence of access requests to the stealth firewall causing said state machine to transition to said final state; and,

upon transitioning to said final state, permitting said network device to access the network protected behind the stealth firewall.

8 A method for permitting access to a network protected behind a stealth firewall comprising the steps of:

receiving a plurality of access requests from a plurality of network devices which are external to the network protected behind the stealth firewall;

not providing a response to said plurality of network device upon receiving each of said access requests;

identifying access request parameters in said received access requests;

performing state transitions in a state machine in the stealth firewall based upon identifying particular ones of said identified access request parameters; and,

upon identifying a pre-determined sequence of access request parameters, said identification of said sequence of access request parameters causing a corresponding sequence of state transitions in the said machine, permitting access to a selected network device responsible for transmitting said sequence of access requests parameters.

9 A method for permitting access to a network protected behind a stealth firewall comprising the steps of:

configuring a state machine to grant access to the stealth firewall contingent upon said state machine transitioning through a plurality of states based upon a sequence of access request parameters identified in received access requests from a single network device;

setting said sequence of access parameters to a specific set of access parameters; and,

disposing said state machine in the stealth firewall.

10 A stealth firewall comprising:

a first network interface to an external network;

a second network interface to an internal network;

a packet filter for restricting access to said internal network, said packet filter ignoring requests from said external network to access said internal network;

fixed storage in which at least one authentication password can be stored;

a hash processor configured to apply a hashing algorithm to said stored at least one authentication password; and,

a comparator configured to compare a hashed password and timestamp received from said first network interface, with a hashed result produced by said hash processor for a stored password associated with a user at said first network interface, said comparator causing said packet filter to permit access to said internal network where said hashed password and timestamp matches said hashed result.

11 A machine readable storage having stored thereon a computer program for permitting access to a network protected behind a stealth firewall, said computer program comprising a routine set of instructions for performing the steps of:

initializing a state machine configured to grant access to the stealth firewall contingent upon said state machine transitioning across a plurality of internal states responsive to receiving a plurality of requests to access the network from a single network device, said plurality of requests collectively comprising a code for causing said state machine to permit access to the network;

receiving an access request from a network device in a network which is external to the network protected behind the stealth firewall, identifying an access parameter in said access request and transitioning from an initial state in said state machine to an intermediate state if said identified access request satisfies transitioning criteria associated with said state machine for transitioning from said initial state to said intermediate state;

receiving a further access request from said network device in said network which is external to the network protected behind the stealth firewall, identifying a further access parameter in said further access request and transitioning from an intermediate state in said state machine to a final state if said identified further access request satisfies transitioning criteria associated with said state machine for transitioning from an intermediate state to said final state;

not providing a response to said network device upon receiving each said access request from said network device in said network which is external to the network protected behind the stealth firewall unless said network device provides a sequence of access requests to the stealth firewall causing said state machine to transition to said final state; and,

upon transitioning to said final state, permitting said network device to access the network protected behind the stealth firewall.

12 A machine readable storage having stored thereon a computer program for permitting access to a network protected behind a stealth firewall, said computer program comprising a routine set of instructions for performing the steps of:

receiving a plurality of access requests from a plurality of network devices which are external to the network protected behind the stealth firewall;

not providing a response to said plurality of network device upon receiving each of said access requests;

identifying access request parameters in said received access requests;

performing state transitions in a state machine in the stealth firewall based upon identifying particular ones of said identified access request parameters; and,

upon identifying a pre-determined sequence of access request parameters, said identification of said sequence of access request parameters causing a corresponding sequence of state transitions in the said machine, permitting access to a selected network device responsible for transmitting said sequence of access requests parameters.

13 A machine readable storage having stored thereon a computer program for permitting access to a network protected behind a stealth firewall, said computer program comprising a routine set of instructions for performing the steps of:

configuring a state machine to grant access to the stealth firewall contingent upon said state machine transitioning through a plurality of states based upon a sequence of access request parameters identified in received access requests from a single network device;

setting said sequence of access parameters to a specific set of access parameters; and,

disposing said state machine in the stealth firewall.

IX. EVIDENCE APPENDIX

No evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 of this title or of any other evidence entered by the Examiner has been relied upon by Appellant in this Appeal, and thus no evidence is attached hereto.

X. RELATED PROCEEDINGS APPENDIX

Since Appellant is unaware of any related appeals and interferences, no decision rendered by a court or the Board is attached hereto.